

SECURING NETWORK SERVICES

After reading this chapter and completing the exercises you will be able to:

- ◆ Plan and implement Windows 2000 DNS and DHCP Security by using features such as secure dynamic updates, secure zone transfers, authorization, and Active Directory integrated zones.
- ◆ Plan a secure implementation of Remote Installation Services.
- ◆ Plan a secure implementation of Terminal Server Services.
- ◆ Plan a secure implementation of Simple Network Management Protocol (SNMP).
- ◆ Implement server security configurations using security templates.
- ◆ Plan and implement secure access for non-Microsoft clients such as Netware, Macintosh, or UNIX/Linux clients.

Windows 2000 offers a variety of network services and features that provide increased functionality and ease the administration of tasks, such as network management and workstation deployment. Although these services can make your task as an administrator significantly more efficient, they also introduce a number of security concerns. As you design the security policies for your network, you have to also plan for the security of these services.

The security implications of these services begin when workstations and servers connect to a network. As a computer boots into its operating system, it must acquire an IP Address. If the IP address is not statically assigned, an authorized **Dynamic Host Configuration Protocol (DHCP)** server is needed to hand out a correct IP address. Once the computer obtains an IP address, the address might need to be registered with the **Domain Name System (DNS)** server so that other computers can locate the services available on the machine. This start-up process creates a number of security issues. Is the client getting the IP address from an approved DHCP server, or has someone installed an illegitimate DHCP server on the network? Is the DNS server valid? Do you want the client computer to be able to register its information with DNS? And how can you make sure that another computer doesn't overwrite the information in DNS?

To assist the administrator with network management, Windows 2000 includes two new features called Remote Installation Services (RIS) and Terminal Services, in addition to a standard implementation of Simple Network Management Protocol (SNMP). **Remote Installation Services (RIS)** provides an automated process for remote deployment of Windows 2000 Professional workstations. Again, this raises some security concerns since you want to insure that only authorized users can install new workstations in the domain. **Terminal Services** enables users to log on to a server and run applications on the server. One configuration of terminal services allows the administrator to log onto a server remotely to perform administrative tasks. Obviously this requires increased security—you want to ensure that only legitimate administrators can log on to the terminal server, and that both the authentication and transmission of the password across a remote connection is secure. **Simple Network Management Protocol (SNMP)** is a network management protocol that sends network and computer configuration information across the network. To secure your SNMP implementation, you need to ensure that this information is sent only to legitimate destinations.

This chapter discusses the implementation and security considerations of network services, such as DNS and DHCP, and administration tools, such as Remote Installation Services, Simple Network Management Protocol, and Terminal Services. The chapter finishes with a discussion on how to secure various types of Windows 2000-based servers, as well as nonMicrosoft clients such as Netware, Macintosh, or UNIX/Linux machines that may need to coexist with your Windows 2000 network.

IMPLEMENTING DNS AND DHCP SECURITY

The **Domain Name System (DNS)** service is used by clients to resolve a computer (host) name to an IP address. DNS traditionally uses a hierarchical, searchable, and static database of computer (host) names and IP addresses. DNS is the only service available that can be used to resolve computers' names to IP addresses on the Internet. For example, when the user types *www.Microsoft.com* as the URL, this name must be converted to an IP address before the client can connect to the host server. The DNS service makes this conversion. The user's computer must be configured with the IP address of a DNS server as part of the TCP/IP configuration settings. The computer queries the DNS server to find the IP address for *www.Microsoft.com*. After the client obtains the IP address, it connects to the host using the IP address.

In most cases, the list of names and IP addresses is maintained in a text file located on the hard drive of the DNS server. This list has to be manually updated whenever any changes are made to the registered records. Keeping the records updated has always been a maintenance task for the DNS administrator.

In Windows 2000, the DNS has been enhanced and is an essential foundation for Active Directory. Active Directory relies upon DNS for its namespace structure and host name to IP address resolution. DNS is also a central store for references to the locations of various network services, such as the Domain Controller and global catalog server. A new

DNS record type called a **Service Record (SRV Record)** is used to locate these network services. Another new feature of DNS in Windows 2000 is the ability to provide **Dynamic DNS** updates to the database. DNS resource records can now be updated automatically by client computers or by other services such as Dynamic Host Configuration Protocol (DHCP). Windows 2000 DNS also includes the ability to integrate and secure the zone file information as part of the Active Directory database. This Active Directory Integrated Zone increases security by removing the physical zone configuration file that is usually stored on the hard drive and moving the information into the Active Directory database.

DHCP has also been enhanced in Windows 2000. In previous versions, DHCP was used mainly to provide clients with IP addresses and various other TCP/IP configuration options, such as DNS and WINS server addresses. DHCP now integrates with DNS to assist in dynamic updates of host records. Because of this integration, it is important to understand how security can be affected when implementing both DNS and DHCP services.

DNS Zones in Windows 2000

Before you can develop an effective security plan for DNS, you need to understand the types of zones that can be implemented in DNS. A **DNS zone** represents a part of the DNS namespace that contains the resource records for a particular DNS domain. For example, a company named Lonestar could have an authoritative DNS server with a forward lookup zone named Lonestar.com. This zone file would hold all of the resource records for the domain, such as computer name records, mail exchanger records, and service records. If a client needs to resolve the IP address for any computer or service in the Lonestar.com domain, the authoritative name server provides the information from the zone files.



A forward lookup zone is used to resolve computer names to IP addresses. For example, to resolve *http://www.lonestar.com* to an IP address, the DNS server would refer to the forward lookup zone. A reverse lookup zone is used to resolve IP addresses to host names. If you need to determine which computer is using IP address 10.10.10.45, the DNS server would use the reverse lookup zone.

There are three types of zones that can be created on a Windows 2000 DNS server:

- **Standard Primary**—All zone information is recorded in a read/write configuration file, stored on the DNS server's hard drive.
- **Standard Secondary**—Any changes made to the standard primary zone file are replicated to this zone file. This replication, which is always a one-way replication from the primary name server to the secondary name server, is called a **zone transfer**. The standard secondary zone is a read-only zone, mainly used for load balancing purposes or backup onto a second DNS server.

- **Active Directory Integrated**—This new type of zone, which is available only in Windows 2000, stores the zone information in the Active Directory database rather than in a text file. There are many advantages to implementing an Active Directory integrated zone. First of all, the DNS replication becomes part of the Active Directory replication, rather than using the zone transfer. Active Directory replication is more efficient and more secure than the traditional zone transfers. Security is also increased when using Active Directory integrated zones, as the zone information is no longer stored in a plain text file, but rather in the Active Directory database. Another advantage is that secure dynamic updates are also enabled when a zone is integrated into Active Directory.

If you implement Active Directory Integrated zone, every Domain Controller that is configured to be a DNS server will receive a full read/write copy of the DNS zone information, in addition to the Active Directory domain information. This means that the zone information can be changed on any DNS server, and the change will be replicated to the other DNS servers. However, this DNS information is replicated only within a single Active Directory domain. In multi-domain scenarios, you may need to create standard secondary zones that replicate the Active Directory integrated zone to another domain. This will insure the availability of another domain's zone information.

One of the most important DNS security problems arises from the way secondary zones and zone transfers are implemented. If an attacker wanted to obtain all resource record information located within a particular zone, she could set up a secondary DNS zone and pull all of the resource information from the primary zone. By default, Windows 2000 DNS servers are configured to replicate zone information to any secondary name server that requests a zone transfer. An attacker could also use a network sniffer to capture zone transfer information. The captured information could reveal all internal resource record registrations, which could then be used to launch an attack.

The first step in securing the DNS server installation is to configure the primary name server to transfer the zone information only to specific secondary servers. To configure this setting, use the following procedure:

1. Open the **DNS** console from the **Administrative Tools** menu and expand the **Forward Lookup Zones** container.
2. Right-click the **zone** and click **Properties**. Figure 6-1 shows the interface.
3. Click the **Zone Transfers** tab.
4. Click **Allow zone transfers** and click **Only to the following servers**.
5. Click **Add** to enter the secondary DNS servers.

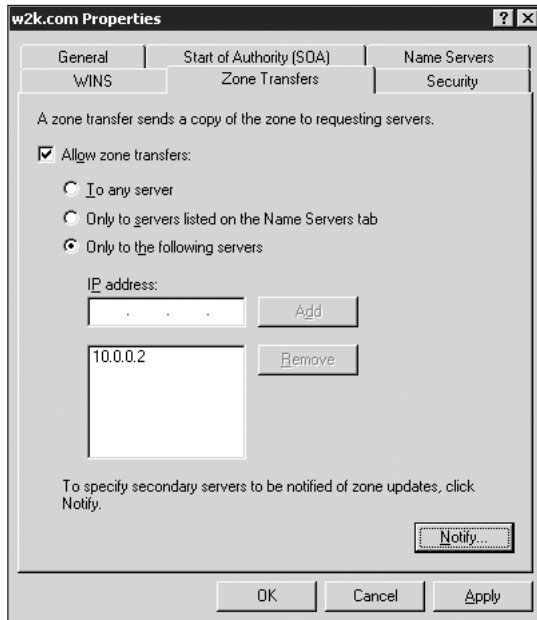


Figure 6-1 Configuring zone transfers to specific DNS secondary servers

By default, all of the zone transfer information is sent across the network in clear text. To protect zone transfers from network sniffers, you need to implement a tool like IPSec to encrypt all zone transfer information. If the zone transfer takes place over a WAN link, VPN technology using Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) with IPSec will secure the transfer from attackers.



IPSec is discussed in detail in Chapter 7, "Securing Network Communications." Configuring VPNs to protect traffic on a WAN link is discussed in Chapter 9, "Securing Access Between Corporate Locations."

The second important security concern with DNS in Windows 2000 involves dynamic updates. In the past, DNS security consisted of controlling access to the DNS server itself, and configuring permissions to allow an administrator to manually edit the resource records. The fact that a Windows 2000 DNS server supports dynamic updates to the resource records changes these security requirements. Windows 2000 DNS allows client machines and DHCP servers to register or remove records automatically from the DNS database. This reduces administrative work because the IP addresses and services can now be registered without any user intervention.

However, dynamic updates are also an important security concern. By default, any Windows 2000 computer can update its resource record with DNS. DHCP can also be configured to update resource records on behalf of clients that cannot update the records themselves, such as Windows 9x, or Windows NT machines. To make this more secure, you should be able to control which clients have the capability to register or change the records in the DNS service. If any client were to update the DNS server records, an attacker could change the resource records for specified computers, thus redirecting network connections to the attacker's computer, or to a nonexistent IP address. Windows 2000 resolves these problems with additional security features built into the DNS service. These features are described in the next sections.

DNS and DHCP Integration Concepts

When you configure dynamic DNS in Windows 2000, you have two options for how client IP addresses will be registered with DNS. The first option is to have clients update their records in DNS. The second option is to use the DHCP server to update the DNS information as part of the process of leasing an IP address to a client.

As a result of this tight integration with dynamic DNS, it is important to understand how DNS updates are performed by the DHCP service. DHCP provides TCP/IP configuration information to workstations. Without DHCP, administrators have to manually configure IP address, subnet mask, and gateway settings for all client machines. With DHCP, this information can be downloaded automatically into the workstation, along with a variety of other options such as WINS and DNS configuration settings.

By default, Windows 2000 client workstations receive their TCP/IP configuration settings from DHCP, and then register or edit their own host record (A record) on the DNS server. In turn, the DHCP server will register the reverse lookup record (PTR record) in the DNS database. If the client workstation is manually configured with the IP information, the Windows 2000 client will update both the A and PTR records itself. Windows 9x and NT machines do not have the capability to dynamically update resource records in DNS. If these clients are using DHCP, the DHCP server can be configured to update both the A and PTR records on behalf of the workstations.

To configure the DHCP server to update DNS on behalf of legacy clients, follow the procedure below:

1. Open the **DHCP** console from the Administrative Tools menu.
2. Right-click the **scope** and click **Properties**.
3. Click the **DNS** tab. Figure 6-2 shows the interface.
4. Click **Enable updates for DNS clients that do not support dynamic updates**.

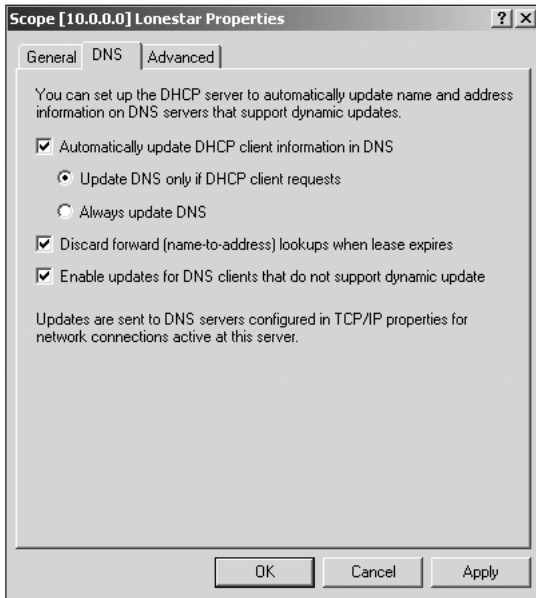


Figure 6-2 Configuring DHCP integration with DNS

The options found on the DNS tab include the following:

- *Automatically update DHCP client information in DNS*—Selecting this option configures the DHCP server to update the client information in DNS. You can then configure server options to define how the DHCP server will do this.
- *Update DNS only if DHCP client requests*—Windows 2000 clients currently request the DNS server to update the PTR record, while the client updates its own A record. Only Windows 2000 clients can make this request.
- *Always update DNS*—This enables the DHCP server to update both the A and PTR records for all clients. This can increase security, because you can configure the security on the DNS database so that only the DHCP server can update the resource records.
- *Discard forward (name-to-address) lookups when lease expires*—Configures the DHCP server to clear forward lookup records for clients when the DHCP lease expires. Selecting this option is a good idea because it will minimize the number of incorrect records on the DNS server.
- *Enable updates for DNS clients that do not support dynamic update*—Select this option to have DHCP update records for preWindows 2000 clients.

A Windows 2000 computer can also be configured not to register its IP address with DNS. You might want to select that option if the DHCP server is configured to update all resource records, or if you did not want to have a particular computer's IP address registered in the DNS database. To configure a Windows 2000 client not to register its IP address, follow the steps below:

1. Right-click **My Network Places** and click **Properties**.
2. Right-click the **network connection** and click **Properties**.
3. Double-click **TCP/IP** and click the **Advanced** button.
4. Click the **DNS** tab. See Figure 6-3.
5. Deselect the **Register this connection's address in DNS** check box.

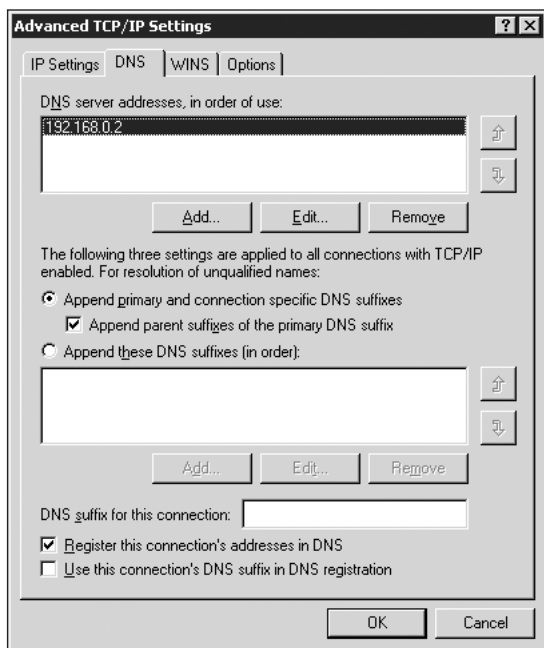


Figure 6-3 Advanced TCP/IP properties

Securing Dynamic Updates to DNS

As mentioned previously, when Windows 2000 clients log onto a network, each client attempts to register its name and IP address with the DNS server. If the client finds that its name and IP are already registered, and if the information differs from the current configuration, it will change the registration to show its current IP. This functionality is desirable in most cases, because a client may receive a different IP address from the DHCP server, and it will need to be able to update DNS. However, this is also a security concern, as any client logging onto the network may be able to change

the other clients' records. This could cause a denial of service for the workstation or, in the case of a network server, the whole network.

The best way to increase the security of the resource records in DNS is to enable secure updates for the DNS zone. Before you can configure a zone for secure dynamic updates, the zone must be Active Directory integrated. Initially, zones can be created as integrated, or can be converted from a primary or secondary zone to be Active Directory integrated.

To convert a zone to Active Directory, follow the steps below:

1. Open the **DNS** mmc from the Administrative Tools menu.
2. Right-click on the zone to be converted and click **Properties**.
3. On the **General** tab (shown in Figure 6-4) click **Change**, and choose the type of zone to convert to.

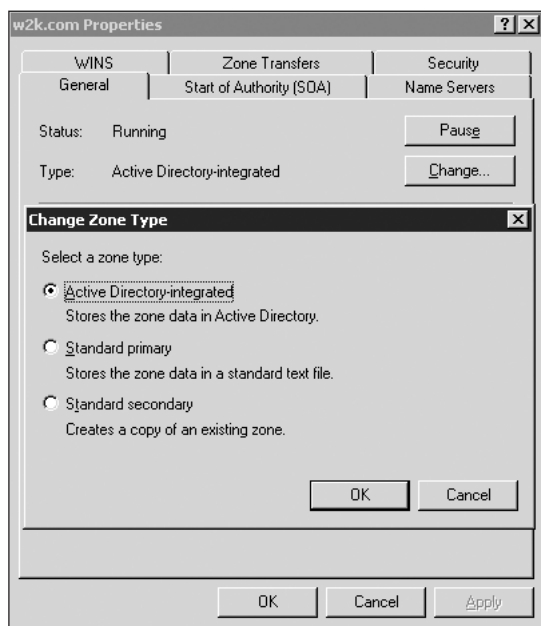


Figure 6-4 Converting a DNS zone to be Active Directory integrated

Once the zone information is integrated into Active Directory, you can enable secure updates. To enable secure updates, follow the directions below:

1. Open the **DNS** mmc from the Administrative Tools menu.
2. Right-click on the zone and click **Properties**. See Figure 6-5.
3. Click the drop-down menu beside **Allow dynamic updates**.
4. Click **Only secure updates**.

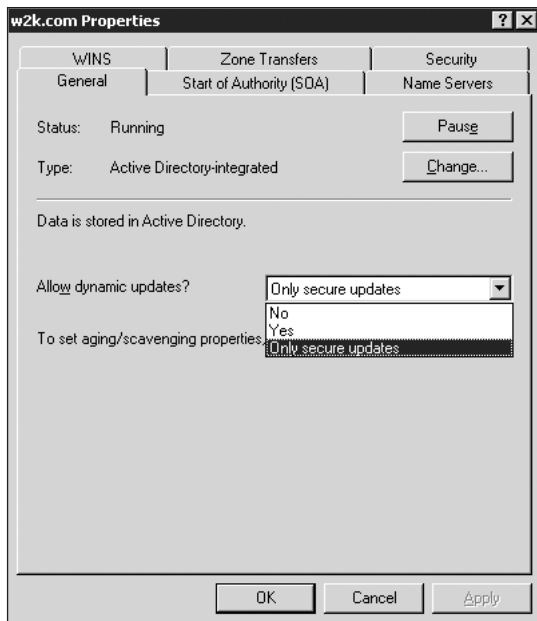


Figure 6-5 Configuring secure updates

Secured zones increase the security of the resource records by allowing only computers that own a record to change the record. The original computer that registers the record becomes the owner of the record. For example, if a Windows 2000 computer named Marketwks receives an IP address from DHCP, it will then register its name and IP address with the DNS server. Marketwks is the owner of the registered record, and only that workstation can modify the record. If the DHCP server registers the records for the clients, as would be the case for Windows 9x or NT machines, the DHCP server itself becomes the owner of the records and is the only computer that can make modifications to the entries.

Configuring a zone for secure dynamic updates also means that only computers with domain accounts can create DNS records. You can even configure additional security, and configure the DNS zone so that only authorized computers and servers will be able to update resource records. Because the DNS zone is integrated with Active Directory, each zone and resource record has an Access Control List (ACL) that can be used to control who has permissions on the particular object. To edit the Access Control List for the zone, use the following procedure:

1. Open the **DNS** mmc from the Administrative Tools menu.
2. Right-click on the zone and click **Properties**.
3. Click the **Security** tab. See Figure 6-6.
4. Edit the ACL to allow or deny security principals the right to create child objects.

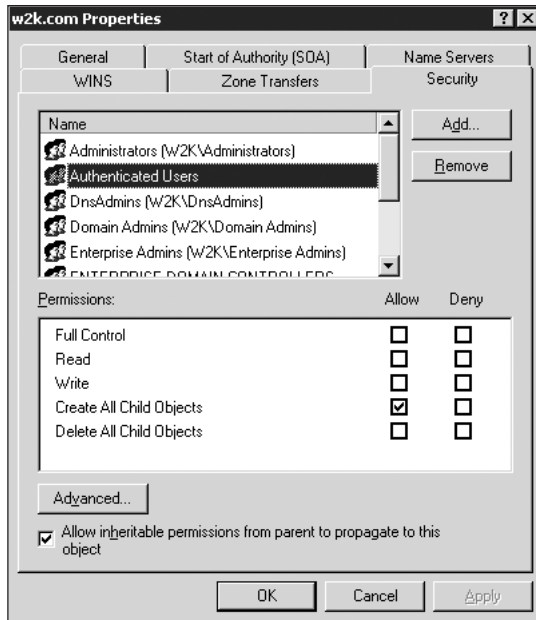


Figure 6-6 Editing the Access Control List on a DNS zone

By default, the **Authenticated Users** group receives **Create All Child Objects** permissions. This means that any authenticated computer or user can create records in the zone. If you want to restrict who is able to update the records, edit the ACL to permit only the authorized users or computers that you select to make changes. Each resource record in DNS also has an ACL that can be edited in the same manner as the zone.

As a Windows 2000 DNS client tries to log on, it first attempts to perform an unsecured dynamic update. If secured updates have been enabled on the DNS server, the client will then perform a second attempt using a secured dynamic update. The secure dynamic update process is as follows:

1. Dynamic updates must be applied to the DNS server that is authoritative for the name to be updated. If the DNS zone is not Active Directory integrated, then the update can happen only on the primary name server. The client will connect to its local name server, which will then refer it to the authoritative server, if the local server is not authoritative.
2. The client attempts to perform an unsecured update. If the zone is configured to allow only secure updates, the server rejects the client's request.
3. The client and server then negotiate a common security mechanism. If both computers are Windows 2000 machines, they will use the Kerberos version 5 protocol. This negotiation is called the TKEY negotiation.

4. The client will resend the dynamic update request, which includes a negotiated key that is used to verify the identity of the sender. This key is called a TSIG key.
5. If the client has the permissions needed to modify or add the particular record, the server will update the resource record. A message is then sent back to the client, along with the TSIG key, to confirm that the update has been completed.

As stated previously, a client always attempts an unsecured update first. You can change this default behavior by adding a new value to the registry. To add this value, follow the steps below:

1. Click **Start**, and then click **Run**. The Run dialog box opens.
2. Type **Regedt32**.
3. Navigate to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters**.
4. Add a new **REG_DWORD Value** called *UpdateSecurityLevel*.
5. Possible data for this value are:
 - a. **0**—Attempt an unsecured update first, and, if it fails, attempt a secure update. This is the default value.
 - b. **16**—Use unsecured dynamic updates only.
 - c. **256**—Use secured dynamic updates only.

One problem that arises when implementing secure dynamic updates involves the use of the DHCP server to register non-Windows 2000 clients with DNS. If the DHCP server is configured to update records on behalf of the Windows 9x or NT clients, the DHCP server becomes the owner of the records. If the down-level clients are then upgraded to Windows 2000, they will not be able to update their own resource records, because only the owner, which in this case is the DHCP server, can make the modifications. In the event of a DHCP server crash, other DHCP servers will also be unable to update a client's information if the IP address changes, because only the original DHCP server owns the records.

To address this problem, put all the DHCP servers into the **DNSUpdateProxy security group**. Objects created by any member of this group have no security, enabling any authenticated user to take over ownership or modify the record. Windows 2000 clients will still be secure because, by default, they will update their own host records.

To add a DHCP server to the DNSUpdateProxy group, follow the procedure below:

1. Click **Active Directory Users and Computers** from the Administrative Tools menu.
2. Click on the **Users** container.

3. Right-click **DNSUpdateProxy** and click **Properties**. See Figure 6-7.
4. Click the **Members** tab, and click **Add** to select the DHCP servers that are to be members of this group.

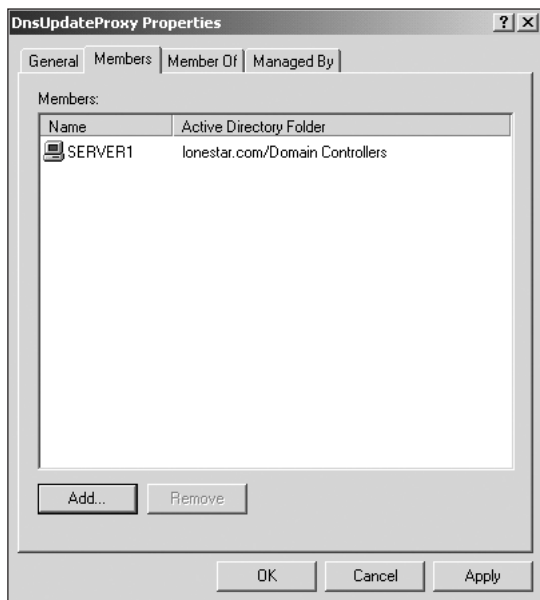


Figure 6-7 DNSUpdateProxy security group properties



If the DHCP server is a Domain Controller, do not add it to the DNSUpdateProxy security group, as any user or computer will have full control of the DNS records on the domain controllers, including the SRV records.

IMPLEMENTING REMOTE INSTALLATION SERVICES SECURITY

One of the new network administration tools included with Windows 2000 is **Remote Installation Services (RIS)**. RIS can be used to simplify and automate the deployment of Windows 2000 Professional to desktop computers. RIS can be used to deploy new installations of Windows 2000 Professional, or to restore dysfunctional systems. It cannot be used to upgrade existing pre-Windows 2000 clients, as RIS formats the hard drive before starting the installation. RIS can automate the entire installation process. For example, if a user's computer fails, she can be given a new computer with no operating system installed on the hard drive. When she turns the computer on, Windows 2000 Professional can be automatically installed from a RIS server. If the RIS image is configured properly, RIS can even install all applications and standard settings required by the

user. The user can start the installation by choosing which RIS image to install, and then simply wait for the installation to be completed with no additional user interaction.

RIS Requirements

Setting up RIS is quite complicated. First of all, to use Remote Installation Services, the following network services must be available:

- *Active Directory*—Needed to help locate RIS servers, prestaged computer accounts, and RIS configuration options.
- *Windows 2000 DNS*—Needed to locate the Active Directory Service through the SRV records.
- *DHCP*—Assigns an IP address to the RIS client.
- *Remote Installation Service*—Is installed as a service on a Windows 2000 server. The RIS server stores the installation images and configuration files that are used by the client. The server hard drive must have at least two partitions, one for the operating system and one for the RIS images. The RIS images must be installed on an NTFS partition.

The RIS clients should meet minimum Windows 2000 Professional hardware requirements. In addition, the workstations also require a network card that supports the Preboot Execution Environment (PXE) remote boot ROM standard, or a network adapter supported by the RIS boot floppy disk. These network cards are needed because, to start the RIS installation procedure, the client must connect to the network to access the RIS server. If the computer has a PXE-compatible network card, the card can connect to the RIS server to download the image. If the client network card is not PXE-compatible, then you will need to use the RIS boot floppy disk to connect to the network.

Configuring RIS

To set up a RIS server, follow the directions below:

1. Click **Start**, point to **Settings**, then click **Control Panel**. The Control Panel window opens.
2. Double-click the **Add/Remove Programs** icon. The Add/Remove Programs dialog box opens.
3. Click **Add/Remove Windows components**.
4. Click **Remote Installation Services** and click **Next**. You may need the Windows 2000 Server CD-ROM to complete the installation.
5. Click **Finish** when prompted. A reboot will also be required to finish the installation.

After installing the RIS server services, you must configure RIS to store the Windows 2000 Professional image and to respond to client requests. To configure RIS, follow the procedure below:

1. Click **Add/Remove Programs** from the Control Panel.
2. Click **Add/Remove Windows Components** and then click the **Configure** button located under **Configure Remote Installation Services**. The RIS setup Wizard will start.
3. Specify a location for the RIS images. This location must be on a separate partition from the operating system and on an NTFS partition.
4. Choose whether to enable the option to have RIS respond to clients immediately after the configuration.
5. Specify a path to the Windows 2000 Professional installation files. You will also be prompted to supply a folder name for the newly created installation point.
6. Enter a description of the installation image. This is used on the RIS installation to enable clients to know which image to select.
7. Click **Finish**. The installation process then creates the installation point and copies the Windows 2000 installation files to the network share. Click **Done** when prompted. (*Note:* Click **Yes** to accept any warnings or prompts that may appear.)

Installing Windows 2000 Professional Clients Using RIS

There are two ways to install a client using Remote Installation Services. The first method requires the computer to be equipped with a network card that is PXE remote-boot-compatible. If the network card does not have a remote-boot CD-ROM, then a second method is to create a remote-boot disk, and then boot from it. The main limitation to the boot disk is that it supports only a limited variety of network cards. Both methods incorporate the PXE standard.

The entire RIS installation of Windows 2000 Professional includes a number of steps, as follows:

1. When the client computer begins the boot process, it detects that it has a PXE-compatible network card. If the BIOS settings on the computer are configured correctly, the computer will attempt to connect to a network location to download a boot image.
2. The client attempts to acquire an IP address from a DHCP server. The initial request for an IP address includes the information that the computer is a PXE client. When the client obtains the address from a DHCP server, the server also includes the location for the client boot files on the RIS server.
3. The client downloads the boot files using Trivial File Transfer Protocol (TFTP) and prepares to boot using this image. At this point, the user is prompted to press F12 if the computer should continue to boot using the network boot image.

4. The next item to appear on the client screen is the Client Installation Wizard. This Wizard guides the user through the process of selecting the RIS image to install on the computer.
5. The user is asked to log on with a user name and password. This user name is used by RIS to determine which RIS image the user has access to. The user is presented with a list of accessible RIS images and asked to choose one of them.
6. After the user chooses the image to install, the hard disk on the computer is formatted, and the new operating system is installed.

Securing Remote Installation Services

Implementing remote installation services raises several security issues. If you do not implement any security, anyone can potentially bring a computer into a company, install an operating system and applications, and gain access to the network. Or a user might inadvertently reinstall an operating system on their computer and, in the process, wipe out all current information on their hard drive. Because of these issues, you must plan your security configuration before deploying RIS.

The following is a list of security concerns that the administrator should consider before deploying workstations using RIS:

- How to prevent unauthorized RIS servers from being installed on the network
- How to prevent unauthorized computers from receiving RIS images
- How to prevent unencrypted boot and installation information from being transmitted between the RIS server and the client

Preventing Unauthorized RIS Servers

To prevent unauthorized RIS servers on the network, Windows 2000 requires that all RIS servers be registered and authorized in Active Directory. A RIS server will not respond to client requests until the registration is complete. Remote Installation Servers are authorized using the DHCP console, and a member of the Enterprise Admins security group must perform the registration.



If the RIS service is installed on the same server as the DHCP service, and the DHCP service is already authorized by Active Directory, RIS does not need to be authorized a second time.

To authorize a RIS server, use the following procedure:

1. Open the DHCP management tool from the Administrative Tools menu.
2. Right-click the **DHCP root** and choose **Manage Authorized Servers**. See Figure 6-8.
3. Click the **Authorize** button and add the IP address or name of the RIS server to be authorized.

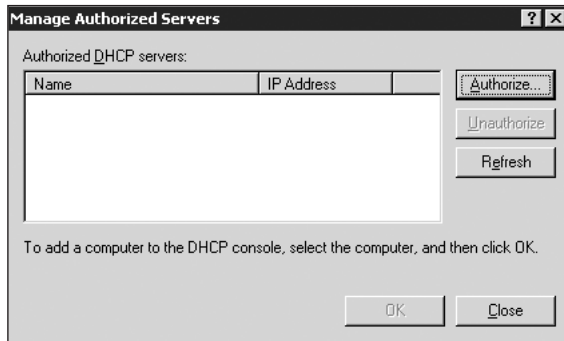


Figure 6-8 Managing authorized RIS servers

Preventing Unauthorized Installation of Computers

The second security concern is ensuring that only authorized computers can install the RIS images. You can use a variety of methods to restrict the installation of computers by setting permissions for both computer and user accounts. When RIS is initially installed, you have the option of enabling or disabling whether RIS will respond to client requests when the installation is complete. Before the RIS server will respond to client requests, this option needs to be enabled. If you did not configure the server to respond to client requests during the installation, you can do so after you have completed the RIS server configuration. To enable the server response, access the RIS server Properties in Active Directory by following the steps below:

1. Click **Active Directory Users and Computers** from the Administrative Tools menu.
2. Click the **Domain Controllers** container and right-click the RIS server object. Click **Properties**.
3. Select the **Remote Install** tab. (See Figure 6-9) To increase security, make sure to also select **Do not respond to unknown client computers**.

If you choose this option, you must also configure **Prestaged Clients**. A prestaged client is a computer account that is created in Active Directory before the computer is installed with the operating system. To successfully prestage a client, you must first determine the computer's globally unique identifier (GUID). The GUID can usually be found either in the system BIOS or on the computer case. The GUID can also be discovered by starting the RIS install and writing down the autogenerated GUID that appears in the setup screen.

Once you have located the computer's GUID, you can prestage a client computer using the following procedure:

1. Open **Active Directory Users and Computers** from the Administrative Tools menu.
2. Create a new computer account in the appropriate container. If RIS is installed in the domain, you are given a choice of creating a managed computer account. See Figure 6-10.

3. Select **This is a managed computer** and type the **GUID** in the indicated text box.

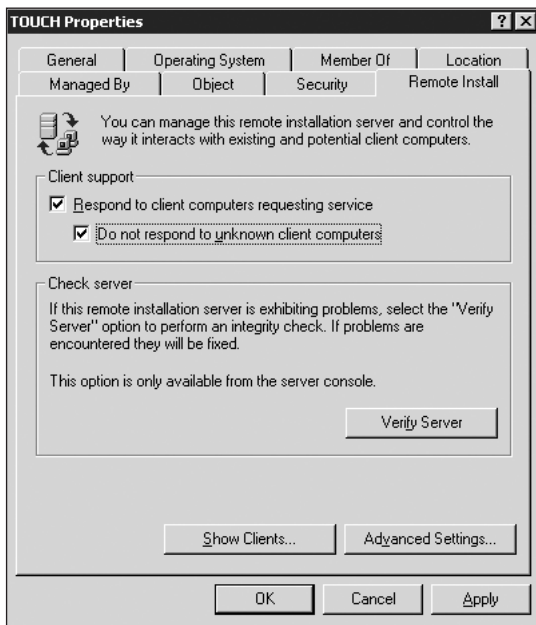


Figure 6-9 Configuring the RIS server properties

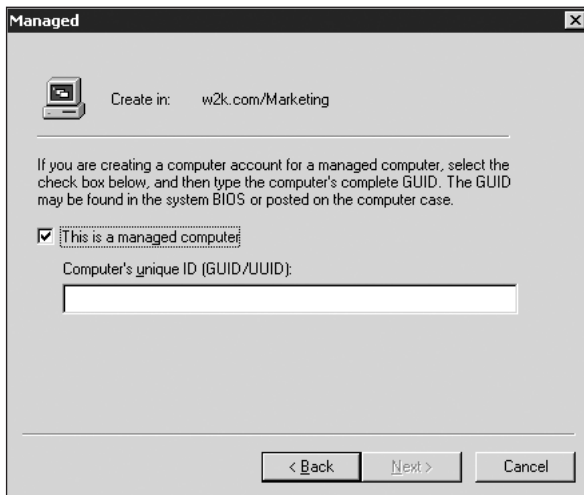


Figure 6-10 Creating a managed computer

Using prestaged computers to restrict the installation of RIS images can require a great deal of administrative effort. For most computers, the only way to determine the GUID

is to actually begin a RIS installation, and then copy down the GUID that appears early in the install. While using prestaged computer accounts is the most secure option for RIS, you can enhance the default security in a number of other ways. These include configuring options, such as where computer accounts will be created, setting computer naming schemes, controlling which images are available for download, and applying DACL permissions to the image files.

To configure RIS installation options, use the following procedure:

1. Open Active Directory Users and Computers.
2. Right-click the **RIS** server and click **Properties**.
3. Select the **Remote Install** tab, and then click **Advanced Settings**. See Figure 6-11.
4. Choose the naming format and client account location.

6

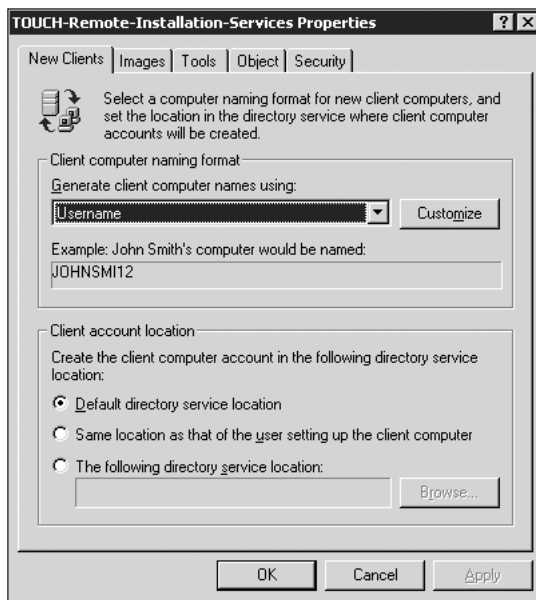


Figure 6-11 Configuring the RIS server advanced settings

Another way to enhance the security of RIS is to limit who can create a computer account in the Active Directory domain. For a user to be able to install a computer account in Active Directory, the user must have Read permission and Create Computer Account permission in the Organizational Unit where the computer account is being created. The easiest way to give a user this level of permissions is to run the Delegation of Administration Wizard and give the user the right to Join a Computer To The Domain.

If you want to limit which RIS images a user can install, you can configure the DACL on the RIS image. By default, all users can install any image available on the RIS server.

The administrator can edit the DACL for the image template to allow only authorized users to install the image. The image's template folder can be found at *<image name>\I386\Templates*.

You can use a combination of these options as you implement RIS security. If you have some computers that require enhanced security, you can prestage those computer accounts to strictly control the RIS installations. For less secure environments, you may be able to simply define the computer names and the location where computer accounts are created. If you base the computer name on the user name and install all computer accounts in the same OU, you can easily determine how many computers have been installed, and who installed a computer. Most large organizations have a limited number of people who can actually create a computer account in the domain, so only these people will be able to install the computers using RIS. If you want any user to be able to install the operating system, but you have distinct images for different departments, then you can use the DACL on the images to control which images appear as options for the users in the different departments.

Securing the RIS Network Transmission

Remote Installation Services uses **Trivial File Transfer Protocol (TFTP)** to transfer logon information, boot files, and installation files. TFTP transfers data in clear text, which can be easily captured and viewed using a network sniffing utility.

Since the data is transmitted in clear text between the RIS server and the client, avoid using an administrator account to install RIS images. A better option is to create a new account with limited privileges in Active Directory. This becomes the installation user account.

IMPLEMENTING TERMINAL SERVER SECURITY

Another important option that is provided with Windows 2000 is **Terminal Services**. Terminal Services offers a new way to provide application support to the computers on a network. Instead of having all the applications installed on each desktop computer, you can install an application on a terminal server and have all the client computers connect to the terminal server to run the application. All of the processing for the application takes place on the server, and only screen write and key stroke information is sent across the network between the server and client.

Terminal Services can be used in two ways in Windows 2000. One way is for remote administration. An administrator can install terminal services on a Windows 2000 server, and then connect to the server from any client computer and run the server or network administration tools. In addition to remote administration, Terminal Services can also provide remote application services where specific client applications are run on the terminal server. In either case, all processing, application storage, file storage, and administration take place at a central server, while clients connect to this server by a thin client console.

Terminal Services allows users who do not have Windows 2000-based computers to use software that requires Windows 2000 and test out the new technology. Users would be able to run this software without having to install the operating system or application on the local computer. For example, an administrator can set up a terminal server with Office XP and then allow users to terminal into the server and test out the new features of the XP product. These users may not have the hardware to be able to install the software locally, so Terminal Services would allow the users to learn and evaluate the new software. Terminal Services clients can include Windows 3.x, Windows 9.x, and Windows NT machines.

A terminal server can be deployed in one of two modes:

- **Application server mode**—Applications are installed on a terminal server, and the client computers connect to the server to run the applications. Client Access licenses must be available for each user connecting to the Terminal Server.
- **Remote administration mode**—Used to provide remote administration capabilities to Windows 2000 Servers. Only members of the Administrators group can connect to the terminal server. This mode includes two remote administration client access licenses.

To install Windows 2000 Terminal Services, use the following procedure:

1. Click **Add/Remove Programs** from the Control Panel.
2. Click **Add/Remove Windows Components**.
3. Scroll until the Terminal Services and Terminal Services Licensing check boxes appear. See Figure 6-12.

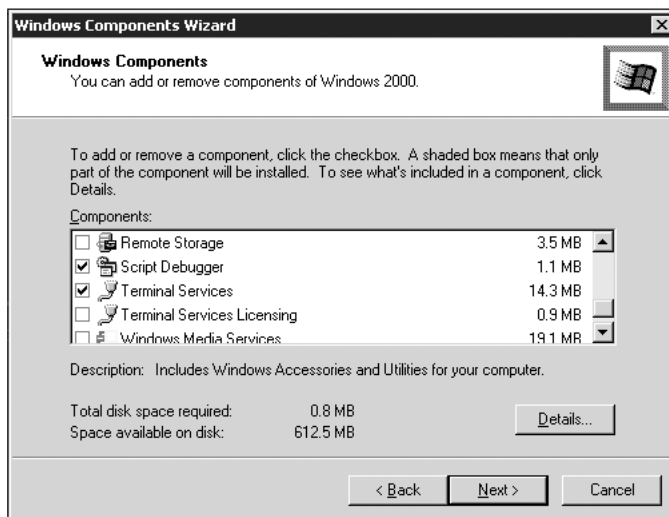


Figure 6-12 Installing the Terminal Services components

4. Select **Terminal Services**, and then click the **details** button. The details screen will allow you to choose whether to install the client creator setup files. See Figure 6-13. Click **OK**.

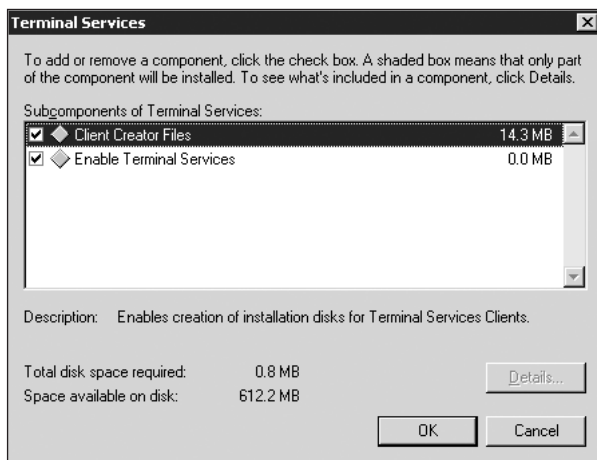


Figure 6-13 Installing the client creator files

5. If you are installing Terminal Services for the purpose of remote administration, make sure that Terminal Services is selected, and then choose **Next**. If installing for the purpose of application sharing, you must also select **Terminal Services Licensing**.
6. On the next setup screen, choose whether you are installing in **Remote administration mode** or **Application server mode**. See Figure 6-14.

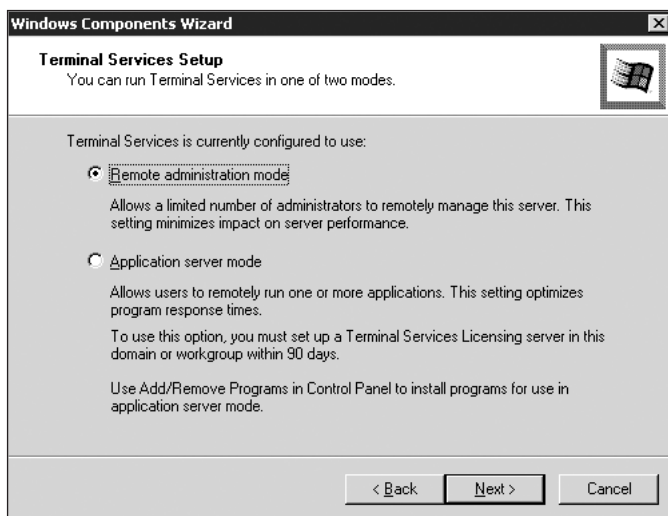


Figure 6-14 Choosing the Terminal Services mode

7. Click **Next** and finish with the Terminal Services setup Wizard. The steps of the Wizard will vary depending upon which mode is selected in Step 6.

If the Client Creator files were installed during the Terminal Services setup, they will be placed in the %systemroot%\system32\clients\tsclient folder on the server. To install the client files on a workstation or thin host, connect to the tsclient folder, choose the appropriate platform (Win32, Win16, etc.), and run the setup program.

Securing Terminal Services

It is essential to secure access to a terminal server. Terminal Services is a powerful tool, but with important security concerns. When a client connects to a terminal server, the client application is running on the terminal server. If permissions are not granted appropriately, the client may be able to delete files on the server hard disk, or change settings on the server, or shut down the server. There are many security issues that you need to plan for when you are implementing terminal services, including the following:

- Remote Access security
- Local File System security
- Transmission security

Remote Access Security

If Terminal Services is installed in Remote administration mode, only members of the Administrators group can connect to the terminal server. Remote administration mode also restricts the number of simultaneous connections to a maximum of two connections.

In some cases, you may want to allow users other than administrators to log into the terminal server. For example, you may have given a user other than an administrator the right to reset passwords in a particular OU, and you may want the user to connect to the terminal server to perform this task. To edit the users or groups allowed to log onto a terminal server configured in Remote administration mode, use the following procedure:

1. Click **Terminal Services Configuration** from the Administrative Tools menu.
2. Select the **RDP-Tcp** connection, right-click, and click **Properties**.
3. Select the **Permissions** tab, and edit the ACL to allow or deny permissions to the terminal server. See Figure 6-15. The three permissions available are:
 - a. *Full Control*—Allows full control of a session, including administering other sessions, remote control, and sending messages to other sessions.
 - b. *User Access*—Allows logging onto a session, sending messages to other users, and querying information about other sessions.
 - c. *Guest Access*—Allows only logging onto a session.

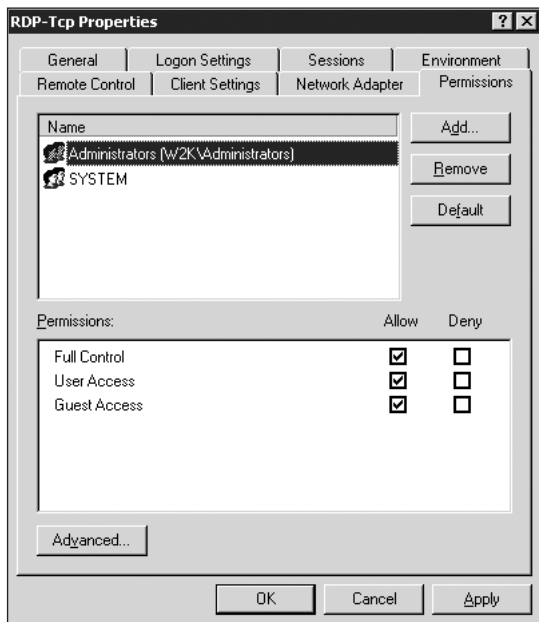


Figure 6-15 Configuring Terminal Services connection permissions



If you are running a terminal server in Application server mode, you can also use this procedure to control who can connect to the server. In addition, you can control which users can use Terminal Services through Active Directory.

Any user that logs on locally or through an RDP connection automatically becomes a member of the **Terminal Services Users group**. Administrators can use this built-in group to control access to local resources on the terminal server. A better security method may be to apply the *Notssid.inf* incremental security template. This template removes the Terminal Server Users group from all DACLs on the file system. This will ensure that user access to resources on the server will be based on actual user and group memberships, and not on the Terminal Servers Users group. More information about security templates will be discussed later in the chapter.

Local File System Security

All terminal server clients log on locally to the terminal server when they connect to the server. Just like a personal workstation, the client has the potential to access any files or folders on the local hard drives of the server. If permissions are not configured carefully, one user may be able to access and change another user's files. Or the user may be able to delete files required by another user. The first step to making this more secure is to use only NTFS partitions on the terminal server. In most cases, you should also insure that user-specific files (such as the user profile or home directory) and data files are actually stored on a file server separate from the terminal server. As much as possible, the users

should have only read permission files on the terminal server—any files that the user can modify should be located on another server where it is easier to protect access to the files. Some applications may require that the user have the right to change some files on the terminal server, so you will have to test each application that you install. In every case, you should try to grant as few permissions as possible to users on the terminal server.



Terminal Services clients also share service access on the terminal server. For example, if a connected user connects to the Internet using Dial-Up Networking, all other terminal-based users will be able to access this connection.

Terminal Services clients require Log on Locally rights on the terminal server to be able to connect to the server. With this in mind, be careful not to deploy Terminal Services in Application server mode on a domain controller. If Terminal Server in Application server mode is deployed on a DC, all terminal services clients would be able to access the server and log on locally to all Domain Controllers in the domain. For security reasons, Application server mode should be deployed only on member servers in the domain.

6

Transmission Security

Another issue that you need to plan for is the security of the information that is sent between the client and the terminal server. Windows 2000 terminal services uses the **Remote Desktop Protocol (RDP)** to carry communication between a server and client. By default, the data is encrypted when using the Remote Desktop Protocol. The data encryption level can be adjusted to meet the security requirements of the corporation.

To adjust the encryption level, use the following procedure:

1. Click **Terminal Services Configuration** from the Administrative Tools menu.
2. Select the **RDP-Tcp** connection, right-click, and click **Properties**.
3. Click the **General** tab. See Figure 6-16.
4. Adjust the **Encryption level** from the drop-down menu.

You have three options when setting the encryption level:

- *Low Encryption*—Encrypts only traffic from the client to the server. Traffic from the server to the client is not encrypted. Data is encrypted using the RC4 algorithm and either a 56-bit or 40-bit key.
- *Medium Encryption*—Encrypts all data sent in both directions between the client and the server. Data is encrypted using the RC4 algorithm and either a 56-bit or 40-bit key.

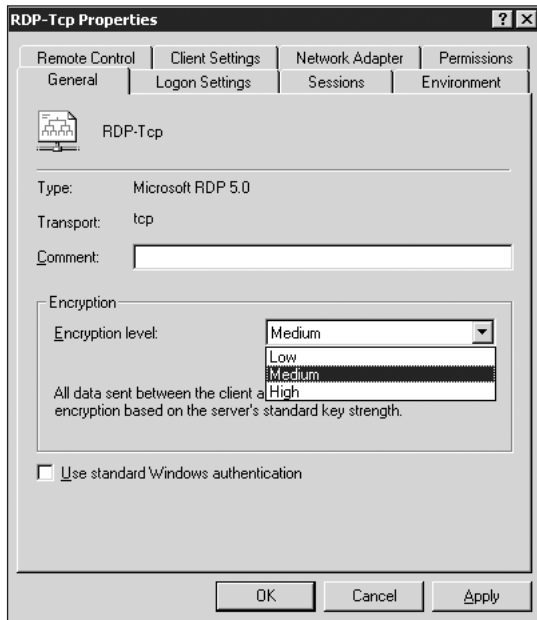


Figure 6-16 Adjusting the Terminal Services encryption levels

- *High Encryption*—Encrypts all data sent in both directions between the client and the server. Data is encrypted using the RC4 algorithm and a 128-bit key. This level requires the installation of the Windows 2000 High Encryption Pack or Windows 2000 Service Pack 2.

IMPLEMENTING SNMP SECURITY

Simple Network Management Protocol (SNMP) is used to assist an administrator in managing and configuring network resources. Administrative tasks such as network performance monitoring, usage auditing, and remote configuration can all be accomplished using SNMP. Specific events can also be monitored and reported, such as device failures or an attempt to take over a particular device. SNMP administration consists of two main concepts: SNMP agents and SNMP management stations.

An **SNMP agent** is a service that runs on a device and collects information about that device. This information can then be reported as status messages to a management station. For example, you may install an SNMP agent on a router, and the agent will collect the performance and configuration data for the router. Then the information is sent to a management station, where the data is stored and displayed for the administrator. In some instances, the agent may also allow configuration changes to be made on the device. An administrator may configure the agent to send an alert message called an **SNMP trap** whenever specific events take place. For example, an administrator may configure a router

to send an alert to the management console whenever a certain percentage of packets or specific number of packets have been discarded at the router interface. Another example could be a trap configured to alert the administrator whenever someone attempts to take control of the agent using an unauthorized management station.

The **SNMP management station** is the central administrative point that allows the administrator to query, monitor, and receive status messages from any SNMP agent configured on the network. The information collected by SNMP agents includes a variety of internal configuration and performance information. As well, the agent can be configured to allow remote configuration changes to network devices. This information must remain secure to ensure the integrity of the network resources. Configuring security for SNMP includes the following components:

- Allowing SNMP community memberships
- Allowing only authorized management stations
- Securing the transmission of the SNMP status and trap messages

Securing Community Memberships

SNMP communities are a collection of SNMP agents that are all managed together as a group and that all have a common community name. In most cases, each SNMP community also has designated SNMP management stations for the community. An agent can belong to more than one community to allow multiple management stations to request information, although an agent will not respond to any management station that is not a member of its community.

Each community that the agent belongs to can have various management rights assigned to it. These rights include the following:

- *None or Notify*—The agent will discard all requests from management stations and send an authentication trap to the management stations in the community that it belongs to.
- *Read Only*—The agent processes only information-gathering commands from the management station, such as GET, GET-NEXT, and GET-BULK.
- *Read Create or Read Write*—The agent allows the processing of all information including SET requests. SET requests allow remote configuration of the device.

When SNMP agents are first installed, a default community name is created named Public. Many administrators leave this default name, mainly for convenience. Since this default community name is well known, it is important to create a new name that is difficult to guess. Any communities that the agent belongs to should be listed in the Accepted community names list with the appropriate permissions. Figure 6-17 shows the interface where this option is configured on a Windows 2000 server.

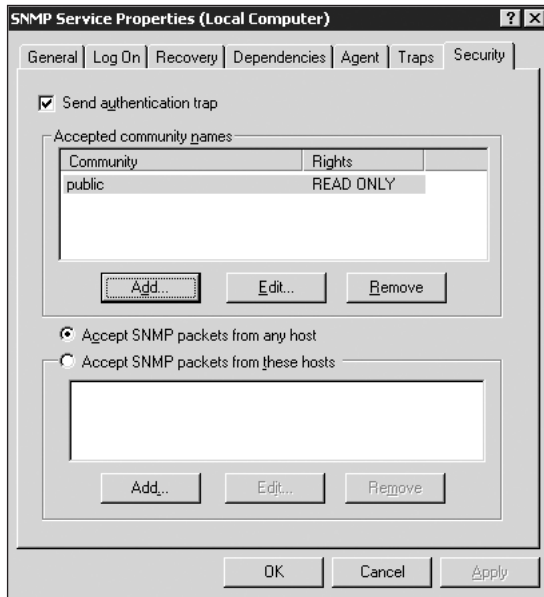


Figure 6-17 Configuring SNMP communities and security



The SNMP service is not installed by default on Windows 2000 computers. You can install the service through Add\Remove Windows Components under Add\Remove Programs in the Control Panel. The Simple Network Management Protocol is located under the Management and Monitoring Tools. After you install SNMP, you can configure the SNMP settings by clicking **Services** in the Administrative Tools menu. You can then right-click the **SNMP Service** and click **Properties**. Various configuration settings will be available as discussed in the section that follows.

Authorizing Management Stations

Security for SNMP can also be enhanced by listing only specific management station IP addresses in the Accept SNMP packets from these hosts section of the SNMP Services Properties dialog box. This will insure that only specific machines will be able to configure or retrieve information from agents belonging to the same community. If an unauthorized attempt is made to connect to an agent, an authentication trap can be sent to specific management stations to warn of the event. This is configured by selecting the Send authentication trap check box on the Security tab.

To make sure that only specific machines receive the traps, follow this procedure:

1. Select the **Traps** tab in the SNMP Services Properties.
2. Choose the appropriate community name.
3. Add specific IP addresses for the management stations that should receive the message. See Figure 6-18.

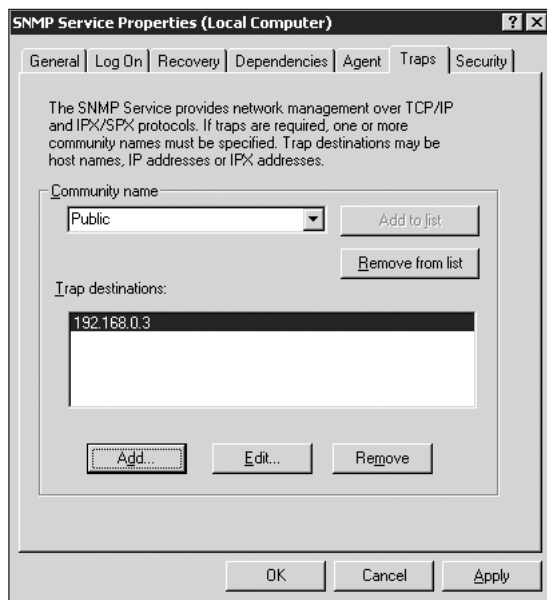


Figure 6-18 Configuring SNMP trap destination

Securing SNMP Transmissions

Another security concern when implementing SNMP is the transmission of the SNMP status and trap messages. These messages could contain confidential data regarding the internal network configuration and status. SNMP sends these messages in clear text, which can be easily captured and read using a network sniffing utility.

The only way to ensure that the data is protected as it is sent across the network is to use IP Security (IPSec). You can deploy IPSec and require that all agents encrypt SNMP status and trap communications between themselves and the management stations. All hosts and management stations must be able to support communication using IPSec encryption technology. Chapter 7, "Securing Network Communications", will discuss IPSec in more detail.

SECURING SERVERS USING SECURITY TEMPLATES

Management of the security settings for a large number of servers and workstations can require a great deal of administrative effort. One way to decrease this effort is to use security templates to manage the security settings on large groups of computers at one time. Security templates can be used by administrators to quickly define and apply various security settings to the domain controllers, servers, and Windows 2000 clients within the domain. Templates can be created and configured using the Security

Templates snap-in or by creating a Group Policy Object in Active Directory. Templates can also be used to check and modify the security settings on a computer by using the Security Configuration and Analysis snap-in.



Chapter 4, “Securing Active Directory” described the procedures for designing security templates and applying these templates by using group policies and Active Directory. Most of the examples discussed in Chapter 4 involved Domain Controller security settings. In this chapter, we will take a closer look at how security templates can be used to secure servers and workstations. The procedures for implementing the templates are the same as discussed in Chapter 4.

Default Security Settings

The first step in configuring and implementing security templates is to categorize the network computers into three main categories: workstations, servers, and domain controllers. These three categories relate to the default security templates included with Windows 2000, although an administrator can design a custom template. Keep in mind that only Windows 2000-based computers can take advantage of security template configurations and deployments.

It is essential to understand the security differences between a newly installed Windows 2000-based computer and one that has been upgraded from Windows 9x or NT. When Windows 2000 is installed as a fresh install on an NTFS partition, a basic template is applied that increases security on specific folders, such as the %systemroot%, and the system registry. Computers upgraded from Windows NT maintain their previous security settings, and do not receive the increased security on the folder's or registry's access control lists.



Windows 9x computers upgraded to Windows 2000 will have the default security settings applied, with the exception that all local user accounts become members of the local administrator's group, if the file system is converted to NTFS. Be sure to review and edit the local administrator's group membership after an upgrade.

The Basic Templates

There are three basic security templates that will be applied to a new installation of Windows 2000. The template that gets applied depends on the role of the machine itself.

- *Defltwk.inf*—Applied to Windows 2000 Professional workstations
- *Defltsv.inf*—Applied to Windows-2000-based servers
- *Defltdc.inf*—Applied to Windows-2000-based servers that are promoted to Domain Controllers

These files are stored in the %systemroot%\inf hidden folder. When a template is applied during an installation, the default template is copied, renamed to Setup Security.inf, and placed in the %systemroot%\security\templates folder.

As stated earlier, computers that are upgraded from Windows NT to Windows 2000 do not have any default templates applied. This is to insure that any previous security configurations are still maintained after the upgrade.

The three following templates can be applied to computers after you have upgraded them from Windows NT to “harden” the security settings. The only settings that are not affected are user rights and group modifications, as some applications may need specific rights or group assignments to function correctly.

- *Basicwk.inf*—Applied to computers upgraded to Windows 2000 Professional
- *Basicsv.inf*—Applied to servers upgraded to any version of Windows 2000 server that are not configured as Domain Controllers
- *Basicdc.inf*—Applied to Domain Controllers upgraded to Windows 2000

The Incremental Templates

If the basic security settings do not meet your security needs, you can apply various additional security configurations using **Incremental Templates**. These templates should be applied only to machines already running the default security settings, as they do not include any of the initial configurations that the basic templates apply.

- *Compatws.inf*—This template can be applied to workstations or servers. Windows 2000 has increased the default security considerably over previous versions. In some cases, this increased security causes application compatibility problems, especially for noncertified applications that require user access to the registry. One way to run these applications is to make the user a member of the Power Users group, which has a higher level of permissions than a normal user. Another option is for the administrator to increase the security permissions for the Users group. The Compatws.inf template provides a third alternative by weakening the default security to allow legacy applications to run under Windows 2000.



A utility called Apcompat.exe, which is included in the Windows 2000 support tools, can also be used by an administrator to configure legacy applications to run in Windows 2000. This utility can configure Windows 2000 to emulate a particular Windows operating system environment so that the application can run properly.

- *Securews.inf* and *Securedc.inf*—These templates provide increased security for areas such as account policy, auditing, and registry permissions. The Securews.inf template is for any workstation or server, while the Securedc.inf template should be applied only to Domain Controllers.

- *Hisecws.inf* and *Hisecdc.inf*—These templates can be incrementally applied after the secure templates have been applied. Security is increased primarily in the areas that affect network communication protocols. These templates should be applied only to pure Windows 2000 environments and should be applied to all machines to ensure proper connectivity. The *Hisecws.inf* template is for any workstation or server, while the *Hisecdc.inf* template should be applied only to Domain Controllers.
- *DC Security.inf*—This template is applied automatically whenever a Windows 2000 member server is promoted to a domain controller. It is available to give the administrator the option to reapply the initial Domain Controller security if the need arises.
- *OCFilesw.inf* and *OCFiless.inf*—These two templates increase the local security of optional components such as Internet Explorer, Microsoft NetMeeting, or Internet Information Services. *OCFilesw.inf* should be installed only on standalone or member servers running Windows 2000, while *OCFiless.inf* should be installed only on Windows 2000 Professional.
- *Notssid.inf*—This template removes the Terminal Users security group SID from all DACLS. If this is defined, all terminal server users will have their permissions applied through individual user and group memberships rather than the terminal server access account SID.

The security templates included in Windows 2000 provide the administrator with acceptable security configurations for a variety of situations. If there is a unique situation, in which a preconfigured template does not fit, you can create a custom one. To create a new security template, use the following procedure:

1. In the Security Templates mmc, right-click the **%systemroot%\Security\Templates** node and choose **New Template**.
2. Type in a template name and description.
3. Edit the various categories as needed.



You can also use a preconfigured template as a baseline and save any changes to a new template. In Step 1 above, right-click a preconfigured template, and then choose **Save As**.

IMPLEMENTING SECURE ACCESS FOR NONMICROSOFT CLIENTS

Most of this book has focused on providing security for Windows 2000 servers and workstations. However, many large corporate networks include a mixture of network directory services and may have workstations that use many different operating systems. In some cases, these organizations may be in the middle of a migration. For example, companies in the process of migrating from a Novell to a Microsoft network usually

have a need to integrate and have the two network systems coexist, often for an extended period of time. Other companies have a mixed environment and have no plans of migrating to a single platform. A common example in many large enterprise organizations is the requirement for UNIX-based or Linux-based applications, which will exist along with a Windows 2000 Active Directory structure. Desktop publishing companies often have a large deployment of Macintosh clients.

Most companies with a variety of operating systems require at least some level of interoperability between the different systems. In some cases, the interoperability must be as seamless as possible. Ideally, a user should not be aware of whether a file share is located on a UNIX, Netware, or Windows 2000 server. The user should simply be able to connect to the share and perform the required task. Creating this seamless client environment can require a great deal of administrative effort to insure that all network services are accessible to the required clients. One of the issues that must be resolved when deploying and supporting a variety of network operating systems is maintaining security when authenticating and accessing network resources.

Securing Network Access to UNIX Clients

Many large networks include UNIX servers and workstations. In this environment, Windows 2000 clients may require access to resources located on UNIX servers, and UNIX clients may require access to resources on Windows 2000 servers. To make the integration between UNIX and Windows 2000 as seamless as possible, Microsoft has released Microsoft Services for UNIX version 2.0. This is an add-on product that includes the following components:

- *Network File System (NFS) Software*—NFS is the file system used by UNIX clients. The NFS software included with the Services for UNIX includes Client, Server, and Gateway software. The client software allows Windows 2000-based clients to connect to a UNIX-based server to access file resources by installing an NFS client on the Windows 2000 computer. The server software installs an NFS server component on the Windows 2000 server so that UNIX clients can connect to Windows 2000 servers to access file resources. The gateway software allows Windows 2000-based clients to connect to a UNIX file system through a common gateway such as a Windows 2000 server. In this case, the gateway component is installed on one Windows 2000 server, which then provides the connection to the UNIX server. All the Windows 2000 clients will connect to the gateway server to access the UNIX resources.
- *Administration Tools*—Microsoft Services for UNIX version 2.0 includes a variety of administration tools, such as a Telnet server application, Telnet client application, and a premade UNIX Microsoft management console.
- *Account Management Tools*—Microsoft Services for UNIX version 2.0 includes utilities to assist in the management of accounts between the two directory services. The Network Information System (NIS) Migration Wizard can assist

the administrator in migrating accounts from UNIX to Active Directory. Two-way password synchronization and the User Name Mapping Service both help to consolidate multiple passwords or logons that clients may have to use to access the two network systems.

When a UNIX client connects to a Windows 2000 server, the client must be authenticated before the user can get access to any resources. There are several authentication options available. Which authentication method is chosen usually depends on the UNIX application being used to access the Windows 2000 resource. The authentication methods that are supported include:

- *NTLM*—UNIX clients that use the Server Message Block (SMB) protocol, such as UNIX Samba version 2.0.6 servers, support NTLM authentication. Earlier versions of Samba required clear text to be able to authenticate with Active Directory. SMB is the Microsoft protocol used for connecting to file shares.
- *Kerberos version 5*—UNIX clients can use Kerberos for authentication. Administrators must either configure the clients to use the Windows 2000 KDC or create Kerberos interrealm trust relationships. Either method requires that an account be created in Active Directory and mapped to the appropriate account in UNIX.
- *Certificates*—UNIX clients can use certificates to authenticate to Windows-based Web servers that are using SSL or TLS.
- *Clear Text*—UNIX clients that use TCP/IP utilities such as Telnet might use clear text to authenticate to Windows 2000. Since clear text is very vulnerable to network sniffing, clear text authentication should be incorporated with other technologies, such as SSL or IPsec.

Use the following guidelines when integrating Windows 2000 and UNIX systems:

- Use NTLM or Kerberos version 5, when possible, to protect passwords.
- Encrypt any transmission that may use clear text (FTP, Telnet) with IPsec.

Securing Network Access to Netware Clients

Another common interoperability issue in large corporations is the presence of both Netware and Microsoft networks. In some cases, Netware Directory Services (NDS) may be used as the primary network directory service, with Active Directory used only to authenticate to Windows-based resources or to applications such as Microsoft Exchange 2000 Server. In other organizations, one department or division may be using Netware, while another part of the company is using Microsoft technologies. Other corporations may be in the middle of a migration from one system to the other, a process that can take years in a large corporation. In each of these cases, the Netware and Microsoft technologies may need to interoperate as seamlessly as possible for an extended period of time.

Interoperability between Netware and Microsoft systems involves the possible use of three software services: Client Services for Netware, Gateway Services for Netware, and Services for Netware.

- *Client Services for Netware*—This client software allows Windows-based clients to access resources on Netware servers. Client Services for Netware is installed on each client and provides the protocol and client software to allow the communication. (Client Services for Netware is a Microsoft client that can be used to connect to Netware servers. Most companies that require this connectivity use the Novell client for Windows because it provides more functionality than the Microsoft client.)
- *Gateway Services for Netware*—This server-based software allows Windows clients to access Netware resources through a common connection through a Windows 2000 gateway server. This software is installed and configured only on a Windows 2000 server, and all client access to the Netware resources flows through this server.
- *Services for Netware*—This add-on product provides several utilities, such as File and Print services for Netware (which allows clients running only the Netware client to connect to a Windows 2000 server), a File Migration Utility (used to migrate file resources from Netware to Windows 2000 servers), and Microsoft Directory Synchronization Services (which can be used to migrate user accounts from a Netware directory to Active Directory and to provide some limited account synchronization between the two directories).

Use the following guidelines when integrating Windows 2000 and Netware systems:

- Be aware that Netware servers that use the IPX/SPX protocol advertise their services using Service Addressing Protocol (SAP). This may provide information for attackers about what services are available on the network and which servers are providing the services.
- Be careful to keep up with security policies when attempting to manage and control multiple accounts between Netware and Windows 2000.
- Remember that Gateway Services for Netware uses a single user account between the gateway server and the Netware server when accessing Netware resources. User-level permissions are not available using this method.
- File and Print Services for Netware may store passwords in clear text, posing a possible security risk.

Securing Network Access to Macintosh Clients

The third operating system that is used on many networks is Macintosh. Macintosh clients can access resources on Windows 2000 servers by utilizing the AppleTalk network integration services. These services include the following:

- *File Services for Macintosh*—These services enable Macintosh clients to access files on a Windows-2000-based server.

- *Print Services for Macintosh*—These services allow Macintosh clients to send print jobs to print devices attached to Windows-2000-based servers.
- *AppleTalk Protocol*—The AppleTalk Protocol is the proprietary protocol for Macintosh networks. You can install the Microsoft implementation of AppleTalk on a Windows 2000 server. More often, however, you will just configure the Macintosh computers to use TCP/IP for network communication.

When planning integration and security for Windows 2000 and Macintosh networks, keep in mind that, by default, Macintosh clients are configured to use clear text passwords when accessing resources. When implementing File Services for Macintosh, administrators may use enhanced security measures by configuring Apple Standard Password Encryption or the Microsoft User Authentication Module (MS-UAM). Apple Standard Encryption enables encrypted passwords up to eight characters in length. MS-UAM allows encrypted passwords up to a maximum of 14 characters in length. This method requires that the AppleShare client version 3.8 be installed on the Macintosh computers.

Use the following guidelines when integrating Windows 2000 and Macintosh systems:

- When using File Services for Macintosh, set volume passwords on shared file resources to increase security. Note that this will require Macintosh clients to type in a password; Windows-based clients will not be restricted by volume passwords.
- Keep in mind that Macintosh networking does not support any security for printing. Macintosh printers do not have any user-level or authentication security.

PLANNING BEST PRACTICES

- Use Active Directory integrated DNS zones to take advantage of Active Directory replication and enable secure updates.
- Implement secure updates in DNS to ensure that only the owner of a resource record can modify the record.
- If you need to register the preWindows 2000 clients in DNS, configure the DNCP server to perform the registration. In most cases, however, you do not need to register most of the preWindows 2000 clients in DNS. These clients still require NetBIOS name resolution rather than host name resolution, so it is more important that the clients be registered with a WINS server.
- If you implement secure updates, and the DHCP server is registering down-level clients, place the DHCP servers into the DNSUpdateProxy security group to allow for future upgrades of down-level clients and also to allow other DHCP servers to update a client record.

- To secure DNS zone transfers to secondary zones, specify which secondary servers will be allowed to transfer the information from the primary name server. To insure that the zone transfer information cannot be captured on the network, use VPNs and IPSec.
- To increase security when implementing Remote Installation Services, prestage the computer accounts before installing the operating system.
- Never use an administrator account for remote installation, since TFTP does not encrypt data transmissions. If you use an administrator account, the administrator password will cross the network in clear text.
- Restrict which images a user can choose from when implementing RIS by editing the DACL on the image's template folder. Not only will this decrease the chances of confusion on the part of the user, but you can also prevent the installation of an image that may have software that is inappropriate for a particular user.
- When configuring SNMP, be sure to use a community name that is difficult to guess.
- Because of the weak security within SNMP communities, configure Read Only communities, which will not allow the processing of SET messages.
- Configure Terminal Services to run in Remote Administration mode to allow administrators to remotely administer the server.
- Do not install Terminal Services in Application Server mode on a Domain Controller.
- Implement either medium or high security for a Terminal Services session.
- Be sure to apply the incremental security templates to any machines upgraded from Windows NT.
- If a certain application does not run in the Windows 2000 environment, apply the compatws.inf template to adjust the security settings.

CHAPTER SUMMARY

- DNS and DHCP have been enhanced to provide additional functionality and security in Windows 2000. As clients log onto the network, DHCP will lease an IP address to the client. By default, a Windows 2000 client will update its name and IP address into DNS automatically, while the DHCP server updates the reverse lookup record.
- DNS now incorporates three types of zones: Standard Primary, Standard Secondary, and Active Directory Integrated. Active Directory Integrated zones are the most secure in that the resource records are stored in the Active

Directory database, and replication occurs during the regular Active Directory replication schedule.

- Dynamic updates should be secured to ensure that only clients that are members of the domain can add or update resource records. To secure dynamic updates, the zone must be Active Directory integrated.
- Remote Installation Services (RIS) can be implemented to remotely deploy Windows 2000 Professional installations. To increase the security when deploying images, an administrator can configure prestaged computer accounts, which will be the only accounts that will respond to an RIS installation request.
- RIS can also be secured by delegating to specific users the capability to create computer accounts in Active Directory and by editing the DACL on the image file to allow only specific users or groups to read the image.
- Terminal Services can be installed in one of two modes: Remote administration mode and Application server mode. Remote administration mode allows only members of the administrators group to connect to the terminal server, and it also sets a limit of only two simultaneous logons.
- To secure Simple Network Management Protocol (SNMP), the default community name (Public) can be changed to a more difficult name that will not be guessed easily by attackers. To increase security when using SNMP, configure each community to be read only, and send authentication traps only to authorized management stations.
- Security templates can be used to apply security settings in various server configurations. Machines with a clean install of Windows 2000 or upgraded from Windows 9x will have the basic security templates already applied. Windows NT machines upgraded to Windows 2000 should have the appropriate incremental security template applied after the upgrade.
- The appropriate service add-on should be implemented when integrating between Windows 2000 and nonMicrosoft clients, such as UNIX, Macintosh, or Netware, to insure that proper security is applied.

KEY TERMS

Active Directory integrated zone — A DNS zone that is stored within the active directory.

Application server mode — A mode within Terminal Services that allows clients to run a common server-based application.

DNS zone — Represents a part of the DNS namespace that contains resource records for that zone's DNS domains.

DNSUpdateProxy security group — Objects created in DNS by any member of this group have no security, enabling any authenticated user to take over ownership of the resource record.

- Domain Name System (DNS)** — A hierarchical and searchable database of computer (host) names and IP addresses. Windows 2000 also incorporates SRV records into the database to locate network services.
- Dynamic DNS** — A mode of Windows 2000 DNS that allows clients to automatically enter and modify their own resource records.
- Dynamic Host Configuration Protocol (DHCP)** — A protocol that is used to assign IP addresses and other various options to network clients.
- prestaged clients** — A computer account that is precreated in Active Directory before the operating system is installed on the computer.
- Remote administration mode** — One of the modes available in Windows 2000 terminal servers that is used to provide administrators with remote administration capabilities to Windows 2000 servers.
- Remote Desktop Protocol (RDP)** — The protocol used in Windows 2000 Terminal Services. Only screen write and keystroke information is sent using RDP.
- Remote Installation Services (RIS)** — A service available in Windows 2000 that can be used to simplify the deployment of Windows 2000 Professional to desktop computers.
- secure dynamic updates** — A mode of Windows 2000 DNS that allows Access Control lists to be edited on DNS zones or resource records. This mode also allows only the hosts that own a record to be able to modify the record.
- Service Record (SRV Record)** — A DNS resource record that reveals the name and IP address for special Windows 2000 services, such as the global catalog or site information.
- Simple Network Management Protocol (SNMP)** — Used to assist the administrator in managing and configuring network resources.
- SNMP agent** — A service that runs on a device that reports status messages to an SNMP management station.
- SNMP community** — A collection of SNMP agents that are all managed together as a group and that all have a common community name.
- SNMP management station** — The central administrative point that allows the administrator to query, monitor, and receive status messages from any SNMP agent configured on the system.
- SNMP trap** — An alert message sent to a configured management station.
- standard primary zone** — A DNS zone that stores its read/write database within a text file on the hard drive.
- standard secondary zone** — A copy of the primary DNS zone that is read-only.
- Terminal Services** — A service in Windows 2000 where clients can run applications entirely on a terminal server.
- zone transfer** — The transfer of changes from a standard primary DNS zone file to a standard secondary zone.

REVIEW QUESTIONS

1. Using Active Directory Integrated zones in DNS increases the security of DNS because you can:
 - a. Specify which secondary servers will receive a copy of the zone files.
 - b. Configure which servers will be notified of zone file changes.
 - c. Configure the zone to deny dynamic updates.
 - d. Control which computers can update the resource records in the zone.
2. Which type of authentication can be integrated with UNIX-based networks?
 - a. Kerberos version 5
 - b. certificate-based authentication
 - c. digest authentication
 - d. SSL
 - e. RADIUS
3. How do you prevent unauthorized users from changing DNS records?
 - a. adjust the properties of the Domain Users group in Active Directory Users and Computer
 - b. set the security permissions for the server in Active Directory Users and Computers
 - c. set the security permissions for the server in Computer Management, Services and Applications, DNS
 - d. adjust the advanced properties of the server in Active Directory Users and Computers
4. If you are using a Windows 2000 DNS server and a Windows 2000 DHCP server, the DHCP server can update the resource records for what types of clients?
 - a. Windows 95\98
 - b. Windows NT 4.0 Workstation
 - c. Windows 2000 Professional
 - d. all of the above
5. What configuration option in SNMP controls which management station can read information or change settings on an SNMP agent?
 - a. community name
 - b. username
 - c. groupname
 - d. all of the above

6. Which level of encryption would you choose for terminal server to ensure that all traffic from the client to the server is encrypted?
 - a. low
 - b. medium
 - c. high
 - d. all of the above
7. When a DHCP server dynamically creates a resource record in DNS, the DHCP server is, by default, listed as the owner of the record. If you do not want this to happen, you do you have to do?
 - a. remove the DHCP server from the authorized DHCP server list in Active Directory
 - b. prevent the DHCP server from dynamically creating the resource record
 - c. add the DHCP server to the DNSUpdateProxy group
 - d. stop dynamic updates in DNS
8. You can use Windows 2000 Remote Installation Services to install:
 - a. Windows ME clients
 - b. Windows NT workstation clients
 - c. Windows 2000 Professional clients
 - d. Windows 2000 Servers
 - e. all of the above
9. You want to make sure that only specific computers can use RIS to install new operating systems. What do you have to do to make this possible?
 - a. pre-stage all of the computer accounts
 - b. ensure that the correct permissions are set on the RIS image files
 - c. limit who has access to the Administrator account password
 - d. configure each user account in Active Directory with permissions to install the operating system using RIS
10. You currently have five different images that RIS clients can use to install the operating system on their computers. However, you would like to make sure that the users in the accounting department can only install the Accounting image. What do you have to do to make this possible?
 - a. pre-stage all of the computer accounts and configure which image each computer will receive
 - b. ensure that the correct permissions are set on the RIS image files
 - c. remove all the other images from the RIS server
 - d. configure each accounting user with the right permissions in Active Directory

11. You have decided to deploy Terminal Services on your network so that all of the users running Windows 95 can run a special application written for Windows 2000. After configuring the Terminal Server and installing the client on all the computers, you can connect and run the application. However, the Windows 95 clients cannot connect to the server. What would you check?
 - a. the server connection to the network
 - b. the client version on the Windows 95 computers
 - c. the Terminal Server installation mode
 - d. whether the server is using IPSec
12. What file system should you use on a computer where you are planning to set up Terminal Server?
 - a. NTFS—to make sure that you can secure specific files on the server
 - b. FAT—because your Windows 95 clients need to use FAT
 - c. FAT 32—because you will likely have large partitions
 - d. It doesn't matter which file system you use.
13. In order to ensure that SNMP messages are not captured while being sent across the network, you will need to implement:
 - a. PKI
 - b. packet filtering
 - c. IPSec
 - d. a private community
14. Security templates can be used to:
 - a. Modify the security settings for Windows 2000 Professional computers.
 - b. Modify the security settings for Windows 2000 Server computers.
 - c. Modify the security settings for Windows ME computers.
 - d. Modify the security settings for a standalone Windows 2000 Server.
15. You have 200 Windows 2000 Professional and 10 Windows 2000 Server computers on your network, along with five UNIX servers. You have just acquired Services for UNIX from Microsoft and want to use the software to make it possible for your Windows 2000 clients to move files to and from the UNIX servers. What two options do you have to configure this?
 - a. install the Services for UNIX on a UNIX server and configure it to accept Windows 2000 client connections
 - b. install the Services for UNIX on a Windows 2000 server and configure it as a gateway for the Windows 2000 clients
 - c. install the Services for UNIX client component on each Windows 2000 Professional computer
 - d. install the Services for UNIX server component on a Windows 2000 Server

16. Installing the Client Services for Netware component on your Windows 2000 Professional computer enables you to:
 - a. connect to a Netware server that is running IPX/SPX
 - b. operate as a gateway for other Windows clients trying to connect to a Netware server
 - c. administer a Netware server
 - d. operate as a file and print server for other Netware clients

HANDS-ON PROJECTS

6



Project 6-1

In this hands-on project, you will configure the DNS server to be Active Directory Integrated.

To change the DNS zone type:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **DNS**.
3. Expand **Server1** in the left pane.
4. Expand **Forward Lookup Zones**. Select **Lonestar.com**
5. Right-click **Lonestar.com** and choose **Properties**.
6. On the **General** tab, click the **Change** button next to the Primary Type.
7. Select **Active Directory integrated**. Click **OK**.
8. Click **OK** at the DNS prompt. Click **OK** one more time to return to the DNS console.
9. Right-click **Lonestar.com** and choose **Properties**. The type should now be listed as **Active Directory integrated**.
10. Close all windows and log off.



Project 6-2

In this hands-on project, you will configure secure dynamic updates and view DNS access control lists to determine which users and groups are allowed to make updates to the DNS settings.

To secure dynamic updates:

1. With an administrator account, log on to your Windows 2000 computer.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **DNS**.
3. Expand **Server1** in the left pane.

4. Expand **Forward Lookup Zones**. Select **Lonestar.com**.
5. Right-click **Lonestar.com** and choose **Properties**.
6. Change the **Allow dynamic updates?** selection to **Only secure updates**.
7. Click **OK**.
8. Click the **Security** tab. Note which users and groups are allowed to change DNS settings. Note which group is allowed only read access.
9. Click the **Cancel** button.
10. Close all windows and log off.



Project 6-3

In this hands-on project, you will configure DHCP to update DNS information for all clients that do not support dynamic updates.

To allow legacy client DNS dynamic update support:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **DHCP**.
3. Select and right-click the DHCP server name and choose **Properties**.
4. Click the **DNS** tab.
5. Select the check box next to **Enable updates for DNS clients that do not support dynamic update**. Click **OK**.
6. Close all windows and log off.



Project 6-4

In this hands-on activity, you will install Terminal Services

To install Terminal Services in Remote administration mode:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, point to **Settings**, and click **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. Click **Add/Remove Windows Components**.
5. Enable the checkbox for **Terminal Services**. Click **Next**.
6. Click **Next** to keep the default Remote Administration Mode. If required, insert the Windows 2000 CD-ROM and click **OK**.
7. Click **Finish**. Click **Yes** to restart your server.



Project 6-5

In this hands-on project you will configure Terminal Services to require high encryption, and automatically end an idle session after 10 minutes,

To edit the encryption level of Terminal Services:

1. Log on to your Windows 2000 computer as an administrator.
2. Close any windows that may open in the result of the previous project.
3. Click **Start, Programs**, point to **Administrative Tools**, and click **Terminal Services Configuration**.
4. Click the **Connections** folder.
5. Right-click **RDP-Tcp** and click **Properties**.
6. Change the **Encryption Level** drop-down list box to **High**.
7. To configure an idle session to end after 10 minutes, click the **Sessions** tab.
8. Select **Override user settings**.
9. Change the **idle session limit** to **10** minutes. Click **OK**.
10. Close all windows and log off.

6

CASE PROJECTS



Case Project 6-1

Southdale Property Management has implemented DNS as it is required for Active Directory. At this point, DNS is installed on one of the Domain Controllers, but it is configured as a primary standard zone. You would like to convert the zone to an Active Directory integrated zone, as well as provide some redundancy for DNS. Your manager has asked you to send him an e-mail outlining the reasons for this change and what you would have to change on the network. What would you say in the e-mail?

You have installed Terminal Services in Remote administrative mode on all of the servers in the office. You use this frequently when you are in the office to administer the servers from your desk. You are thinking about configuring the network so that you can also connect to the servers using a terminal session from home so that you do not have to come into the office to troubleshoot problems after work hours. What are the security concerns that you need to address in order to make sure that connecting to the terminal servers from home is secure?



Case Project 6-2

Fleetwood Credit Union is developing a new application that is designed to run on a terminal server. The current plans are to deploy several terminal servers at head office and then install a terminal server client for all the users who need to access the application. The company is also trying to decide whether to deploy the terminal server application onto laptops used by the traveling financial consultants who would then be able to use the terminal server from anywhere to access confidential client information. The manager who is in charge of deploying the application is very worried about security. If this application is deployed to the laptops, it will be used to access confidential client information across an Internet connection. You have been asked to provide an analysis of the security implications for deploying the application to the laptops.